SemPIF : A semantic meta-policy interchange format for multiple web policies

Hu, Yuh-Jong; Boley, Harold

Publisher's version / Version de l'éditeur:
https://doi.org/10.1109/WI-IAT.2010.238
IEEE/WIC/ACM International Conference on Web Intelligence and intelligent Agent Technology (WI-IAT 2010), 3, pp. 302-307, 2010-09-03

SemPIF: A Semantic Meta-Policy Interchange Format for Multiple Web Policies

Yuh-Jong Hu
Dept. of Computer Science
NCCU, Taipei, Taiwan
hu AT cs.nccu.edu.tw

Harold Boley
IIT – e-Business,
NRC-CNRC, Canada,
Harold.Boley AT nrc.gc.ca

***Abstract*—We propose a semantics-enabled layered policy architecture for the exchange and management of multiple policies created by different policy languages on the Web. This architecture consists of four layers: Unifying Logic (UNL), Policy Interchange Format (PIF), Privacy Protection/DRM (PPD), and Domain Specific Applications (DSA). A meta-Policy Interchange Format (meta-PIF) layer is also introduced, side by side with the corresponding PIF layer, allowing agents in the facilitator to provide uniform services of interchange, reconciliation, and combination of policies. This SemPIF architecture extends W3C's Semantic Web architecture to permit the reuse of earlier work. A scenario of agents in the facilitator employing SemPIF for Digital Rights Management (DRM) and privacy protection policies on digital library subscription services will be demonstrated.**

***Keywords*-semantic web; ontology and rule; computer policy; privacy protection; digital rights management**

I. Introduction

In the Semantic Web, information is given well-defined meaning to better enable computers and people to work in cooperation. The well-known Semantic Web layered architecture[1] has undergone revisions reflecting the evolution of layers such as the Description Logic (DL)-based ontology language OWL [1], the Horn Logic (HL)-based rule language RIF [2], and their relationship. On the other hand, policy languages, such as Rei [3], KAoS [4], Protune [5], have also been proposed – on the basis of DL and LP – to allow agents understand policies and to enforce these policies as intended by their semantics. However, the semantic bases of policy languages vary considerably, ranging from DL to HL to Logic Programming (LP), e.g. leading to different stances w.r.t. the unique name assumption (UNA) and the closed world assumption (CWA) [6]. This makes policies created in these policy languages hard to interchange and combine with each other.

Policies are formulated and treated as knowledge bases, i.e. ontologies and rules ($\mathcal{O} + \mathcal{R}$). Many operations can be automated, thereby reducing ad-hoc program coding to a minimum and enabling automated documentation [5]. Policy frameworks also need to support interoperability. Moreover, the context of a policy is itself described in a machine-understandable way. Therefore, we propose a semantics-enabled policy architecture consisting of four layers: Unifying Logic (UNL), Policy/meta-Policy Interchange Format (PIF/meta-PIF), Privacy Protection/DRM (PPD), and Domain Specific Applications (DSA). Here UNL directly corresponds to the layer "Unifying Logic" of the most recent version of the Semantic Web architecture. We also introduce a meta-PIF layer, side by side with the corresponding PIF layer, allowing software agents in the facilitator, to provide the management functions of interchange, reconciliation, and combination of policies. The Policy Web architecture can be viewed as an extension of the Semantic Web architecture shown as Fig. 1.

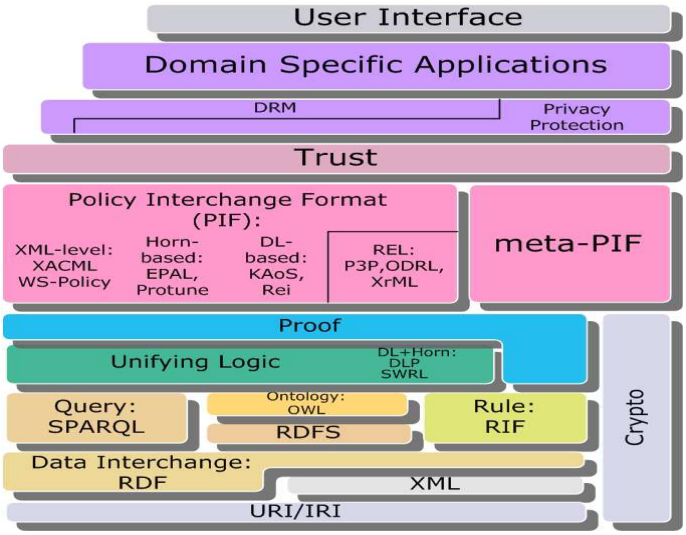

Fig. 1. SemPIF: A semantics-enabled layered policy model centered on semantic policy interchange format (PIF) and meta-PIF.

PIF is built on DL-based ontologies and LP-based rules, i.e. $\mathcal{O} + \mathcal{R}$, that allow agents in the facilitator to support interchange services of policies created from different policy languages. In addition, we may use meta-PIF to specify meta-policies for managing policies created from different policy languages. A meta-policy is a policy about policies that provides a set of rules for realizing services needed for the management of policies. Moreover, a meta-policy consists of a set of rules for setting up the priority of polices to coordinate,

[1] http://www.w3.org/2007/03/layerCake.svg

enforce, and even negotiate policies [7].

In a particular policy language framework, policy management services could be implemented as meta-policies as shown in the Rei framework [3] or it could be implemented as policy administration tools as shown in KAoS [4]. In the Protune framework, the role of meta-policies is in governing the behavior to reduce ad-hoc programming efforts and to improve policy readability and maintainability. However, policy management services in these frameworks were only allowed to operate within their own environments. For added flexibility, SemPIF allows agents in the facilitator to use meta-policies providing the management services of policy interchange, combination, and negotiation across multiple heterogeneous domains.

In contrast to other policy languages, such as KAoS, Rei, and Protune, PIF follows W3C $\mathcal{O}+\mathcal{R}$ standards [8] and strives to provide a mechanism for agents to preserve different policy syntaxes and semantics throughout its policy integration and interchange. In addition, agents can use meta-PIF, providing further management and reconciliation services of PIF-enabled multiple policies across various domains (see Fig. 2).

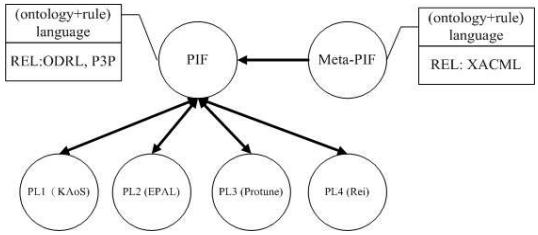

Fig. 2. Policy integration and interchange for various policy languages (PL) through PIF and meta-PIF in the SemPIF

An XML-based Rights Expression Language (REL) lacks semantic expressive power so it is a restricted form of policy language in the PIF layer. Currently, there are three RELs available, i.e. P3P for privacy protection as well as ODRL and XrML for DRM. Unfortunately, policies created from these XML-level RELs lack formal semantics, which prevents agents from automatically and accurately interpreting and processing these policies.

A formal semantic model for policies could be expressed and enforced as a combination of $\mathcal{O}+\mathcal{R}$. Obviously, if we do not know what are the available expressive features of each $\mathcal{O}+\mathcal{R}$ combination, then we cannot decide which combination will be the best one to represent the formal semantics of RELs. We have shown the semantics of DRM policies in PPD as a homogeneous combination of $\mathcal{O}+\mathcal{R}$, i.e. SWRL, where both $\mathcal{O}+\mathcal{R}$ are embedded in a logical language $\mathcal{L}$, to structure the semantics of ODRL [9]. We also have shown the semantics of privacy protection policies in PPD as a hybrid combination of $\mathcal{O}+\mathcal{R}$, i.e. DL+log, where a strict separation between the rule predicates and ontology predicates, to formalize the semantics of P3P in the PIF layer [10].

Another issue addressed by our investigation of the DRM vs. privacy usage control problem is the following. While DRM systems are collecting personal information for usage control, it is quite possible that they might also invade privacy rights. To reconcile this conflict, the $(\mathcal{O}+\mathcal{R})$ language in meta-PIF permits agents to enforce the fine-grained mapping and merging of ontologies with interchangeable rules from policies on privacy protection and DRM. This paves the way for accomplishing the objective of unifying multiple Web policies through SemPIF.

Finally, we will show a scenario for digital library subscription services in a client-server model and demonstrate how to use it by agents in the facilitator to eliminate possible conflicts between a server's DRM policies and a client's privacy protection policies.

II. Semantic Web Layered Architecture

We have both Web markup languages and Semantic Web languages in the Semantic Web Layered Architecture (SWLA) (see Fig. 1). XML / XML Schema and URI/IRI references constitute the foundation, which provides interoperable syntax for RELs at the PIF layer. The semantics of RELs need to be formalized with one of the $\mathcal{O}+\mathcal{R}$ combinations from the UNL, to provide meanings for policies. For Semantic Web languages, we have ontology languages, rule languages, and a combination of ontology and rule languages, i.e. $\mathcal{O}+\mathcal{R}$ languages. The ontology languages include the graph-based RDF(S) and the DL-based OWL. The Horn-based rule languages and their extensions to LP-based rule languages include RIF and RuleML. SWRL is a Semantic Web language using a combination of OWL-DL ontologies and Datalog RuleML rules so it is an $\mathcal{O}+\mathcal{R}$ language [11]. OWL 2 RL and its combination with RIF is another emerging $\mathcal{O}+\mathcal{R}$ language that can be compared with DLP[2].

A. Unifying Logic

PIF and Sem-PIF are built on the unifying logic of DL-based ontologies and LP-based rules [6]. In the UNL layer, DL is a subset of the First Order Logic (FOL). DL provides a basic logic foundation for an ontology language, such as OWL 2. Similarly, Horn logic and LP provides a basic logic foundation for rule languages, such as RIF or RuleML. One of LP's characteristics, procedural attachment, is not included in DL (or FOL) but this feature is very important for the execution of policy's actions.

DLP was introduced as the intersection of DL and LP [12], which has quite limited expressive power when compared to other $\mathcal{O}+\mathcal{R}$ combinations, such as $\mathcal{AL}$-log, $\mathcal{DL}$-log, etc. [13] [14]. The homogeneous $\mathcal{O}+\mathcal{R}$ combination of DL and Datalog provides the logic foundation of SWRL. These combinations of $\mathcal{O}+\mathcal{R}$ have much more expressive power than DLP regarding $\mathcal{O}+\mathcal{R}$, which is needed for Sem-PIF. However, given the ongoing $\mathcal{O}+\mathcal{R}$ research[3], we have not fixed yet any one combination for SemPIF's representation and enforcement requirements.

[2]The combination of OWL 2 and RIF has been shown in http://www.w3.org/2005/rules/wiki/OWLRL.

[3]See, e.g., ONTORULE http://ontorule-project.eu/.

B. Policy Interchange Format

The PIF layer consists of regular DL-based policy languages, such as Rei, KAoS; or Horn-based policy languages, such as EPAL [15], and XML-syntax policy languages, such as XACML [16]. P3P and EPAL were proposed as policy languages for privacy protection in the corresponding client-server and server-server models [17] [18]. As REL sublayer, ODRL and XrML were proposed for designing DRM policies [19] [20]. DL-based or Horn-based logic can be used as foundations to underpin these RELs with explicitly defined semantics for policy languages.

A policy's explicit representation in terms of ontologies or rules depends on what the underlying logic foundation of your policy language is. If policies are created from a DL-based policy language, such as Rei or KAoS, then ordinary policies are shown as $\mathcal{T}\mathcal{B}$ox ontology schemas and $\mathcal{A}\mathcal{B}$ox instances. Otherwise, with policies created from LP-based policy languages, such as EPAL, ordinary policies are sets of rules and facts using unary or binary predicates.

These policy languages in the PIF layer do not fully utilize the syntax and semantics expressive power of OWL or RDF(S) shown in the SWLA. Therefore, we do not expect these policy languages to be able to leverage the power of existing ontology or rule languages. Another restriction is policies created from different policy languages might not be able to interchange or negotiate with each other. This calls for the use of SemPIF to achieve policy interchange, combination, reconciliation, and negotiation.

C. Privacy Protection and DRM

Privacy protection and DRM are introduced as independent but intertwined layers on top of PIF / meta-PIF and the Trust layer (see Fig. 1). This relationship reflects that access rights enforcements for these two domains are closely related with each other. In [21], the authors proposed that a DRM system should consider user-desirable privacy rights indicated in the Fair Information Principles (FIP), such as data collection, retention, use, disclosure, and destruction, etc., when it enforces privacy protection policies. Otherwise, user privacy rights might be violated. A scenario will be demonstrated to show how agents in the facilitator employ SemPIF to integrate DRM and privacy protection policies (see section III).

III. A SCENARIO OF DIGITAL LIBRARY SUBSCRIPTION

Protection policies are created from various policy languages, such as ODRL, P3P, XACML, and EPAL, for enforcing DRM and privacy protection. This access-control scenario is extended from policy-aware access control for the open Web environment [22]. Agents in the facilitator use PIF-based policies to provide services of integrating semantics-enabled protection policies between a client and a server. Moreover, Agents use meta-PIF-based policies to manage policies, which permits clients and a server to compromise on their respective rights and obligations(see Fig. 3).

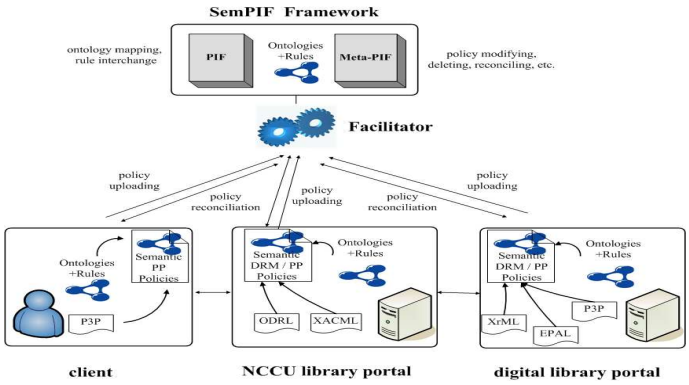

Fig. 3. Agents in the facilitator provide policy interchange services with PIF-based policies and policy management services with meta-PIF-based policies

A. Web server's policies

The $NCCU$ university library has subscribed to $IEEE$, ACM, and $Springer$ digital library services, which provide a set of `eJournal` article access rights for authorized students and staff. There are two types of policy for an IEEE Web server: one for DRM and the other for the declaration of privacy statements.

1) Policies in the IEEE server: The IEEE publisher has two PIF-based policies: $\texttt{policy}(\texttt{drm1}-\texttt{IEEE})$ for DRM and $\texttt{policy}(\texttt{pp1}-\texttt{IEEE})$ for privacy declaration. $\texttt{policy}(\texttt{drm1}-\texttt{IEEE})$ indicates that the policy's name is drm1-IEEE, which corresponds to a URI as a policy indicator for agents to apply a meta-PIF policy to manage it. The predicates of each RIF rule are specified in PIF-based ontologies (see Fig. 4 and Fig. 5).

- $\texttt{policy}(\texttt{drm1}-\texttt{IEEE})$:
  If a student owns a valid student ID issued by a department of a university, e.g. a registrar, and its library is one of the subscribers on the IEEE publisher's list, then the student is endowed with DRM usage rights $\{\texttt{download}, \texttt{view}, \texttt{print}\}$ for `eJournals` from a Web server of the IEEE publisher's delegation.

  $$\begin{aligned}
  &?\texttt{st}\#\texttt{Student}\wedge ?\texttt{id}\#\texttt{StudentID}\wedge ?\texttt{st}[\texttt{own}\rightarrow ?\texttt{id}]\\
  &\wedge ?\texttt{uni}[\texttt{nccuHasPartR}\rightarrow ?\texttt{rg}]\wedge ?\texttt{st}[\texttt{enrolledAt}\rightarrow ?\texttt{uni}]\\
  &\wedge ?\texttt{rg}[\texttt{issue}\rightarrow ?\texttt{id}]\wedge ?\texttt{uni}[\texttt{nccuhasPartN}\rightarrow ?\texttt{lib}]\\
  &\wedge ?\texttt{lib}[\texttt{subscribedTo}\rightarrow \texttt{IEEE}]\\
  &\wedge \texttt{IEEE}[\texttt{hasPublished}\rightarrow ?\texttt{ejr}]\\
  &\wedge \texttt{IEEE}[\texttt{endowedWith}\rightarrow ?\texttt{rgt}]\wedge ?\texttt{rgt}[\texttt{appliedTo}\rightarrow ?\texttt{ejr}]\\
  &\wedge \texttt{IEEE}[\texttt{delegate}\rightarrow ?\texttt{st}]\Longrightarrow ?\texttt{st}[\texttt{endowedWith}\rightarrow ?\texttt{d}]\\
  &\wedge ?\texttt{st}[\texttt{endowedWith}\rightarrow ?\texttt{v}]\ \wedge ?\texttt{st}[\texttt{endowedWith}\rightarrow ?\texttt{p}]\\
  &\wedge ?\texttt{d}\#\texttt{Download}\wedge ?\texttt{d}[\texttt{appliedTo}\rightarrow ?\texttt{ejr}]\\
  &\wedge ?\texttt{v}\#\texttt{View}\wedge ?\texttt{v}[\texttt{appliedTo}\rightarrow ?\texttt{ejr}]\\
  &\wedge ?\texttt{p}\#\texttt{Print}\wedge ?\texttt{p}[\texttt{appliedTo}\rightarrow ?\texttt{ejr}].
  \end{aligned}$$

- $\texttt{policy}(\texttt{pp1}-\texttt{IEEE})$:
  If a person is endowed with DRM usage rights from a Web server of the IEEE's publisher and this publisher has the purpose of enforcing DRM control for collecting,

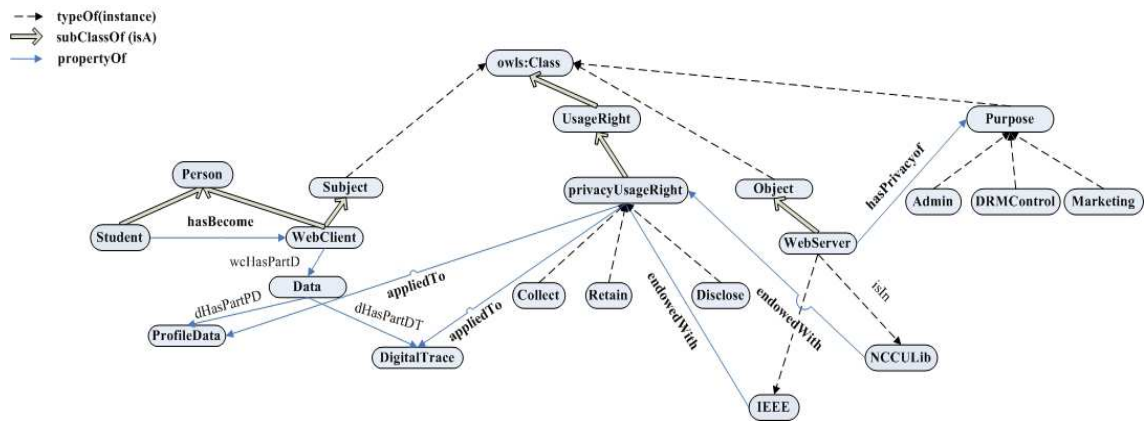

Fig. 4. A PIF-based ontology for privacy protection policies

retaining, and disclosing a person's data, then the IEEE publisher is endowed with privacy usage rights $\{\texttt{collect}, \texttt{retain}, \texttt{disclose}\}$ on this data from a person's delegation, including profiles and digital traces in the Web server under condition of a retention period of two months after the data are first collected.

$$
\begin{aligned}
&?\texttt{per}[\texttt{endowedWith} \rightarrow ?\texttt{drmr}] \wedge ?\texttt{drmr}[\texttt{appliedTo} \rightarrow ?\texttt{ejr}] \\
&\wedge \texttt{IEEE}[\texttt{hasPublished} \rightarrow ?\texttt{ejr}] \\
&\wedge \texttt{IEEE}[\texttt{hasPrivacyOf} \rightarrow \texttt{DRMControl}] \\
&\wedge ?\texttt{per}[\texttt{dHasPartPD} \rightarrow ?\texttt{prf}] \wedge ?\texttt{per}[\texttt{dHasPartDT} \rightarrow ?\texttt{dif}] \\
&\wedge ?\texttt{per}[\texttt{endowedWith} \rightarrow ?\texttt{ppr}] \wedge ?\texttt{per}[\texttt{delegate} \rightarrow \texttt{IEEE}] \\
&\wedge \texttt{Retain}[\texttt{hasDuration} \rightarrow =\text{2Month}] \\
&\wedge ?\texttt{sdtime}[\texttt{dHasPartD} \rightarrow ?\texttt{dtime}] \\
&\wedge ?\texttt{edtime}[\texttt{dHasPartD} \rightarrow ?\texttt{dtime}] \\
&\wedge \text{subtract-dateTimes}(?\texttt{edtime}, ?\texttt{sdtime}) \leq \texttt{Retain} \\
&\Longrightarrow \texttt{IEEE}[\texttt{endowedWith} \rightarrow ?\texttt{ppr}] \\
&\wedge ?\texttt{ppr}[\texttt{appliedTo} \rightarrow ?\texttt{prf}] \wedge ?\texttt{ppr}[\texttt{appliedTo} \rightarrow ?\texttt{dit}].
\end{aligned}
$$

In $\texttt{policy}(\texttt{drm1} - \texttt{IEEE})$, we use ODRL basic primitive vocabularies $\texttt{principal}, \texttt{asset}, \texttt{right}$, or $\texttt{obligation}$ to define a license agreement between principals, i.e., library, registrar, university, and publisher. Similarly, in $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$, we use P3P basic primitive vocabularies, such as $\texttt{user}, \texttt{owner}, \texttt{purpose}, \texttt{rights}, \texttt{obligation}$ to define a privacy protection agreement between data user and data owner. All of the basic vocabularies are defined in the DRM or privacy protection ontology's schema (see Fig. 4 and Fig. 5), so the semantics of ODRL and P3P RELs are formalized. Furthermore, policies specified in other policy languages for DRM and privacy protection can be mapped to the PIF-based policies for the purposes of policy interchange and integration.

2) Policies in a Web client: A student, *John*, as a Web client has privacy protection policies, i.e., $\texttt{policy}(\texttt{pp3} - \texttt{John})$, $\texttt{policy}(\texttt{pp4} - \texttt{John})$ to address how and what of his personal data can (or cannot) be collected, retained, or disclosed from a Web server. Here we show the policies in natural language only.

- $\texttt{policy}(\texttt{pp3} - \texttt{John})$:
  If an `eJournal` distributor from {ACM, IEEE, Springer} has the purpose of enforcing DRM control by collecting, retaining, and disclosing data on John as the Web client, then it is endowed with privacy usage rights $\{\texttt{collect}, \texttt{retain}\}$ on the profiles of John as the Web client under the condition of a retention period of less than thirty days after the profiles are first collected.
- $\texttt{policy}(\texttt{pp4} - \texttt{John})$:
  If the distributor IEEE `Journal` has the purpose of enforcing DRM control by collecting, retaining, and disclosing data on John as the Web client, then IEEE is endowed with the privacy usage rights $\{\texttt{collect}, \texttt{retain}\}$ from the digital traces of John as the Web client, where the data retention period is less than fourteen days after the trace data are first collected.

IV. SemPIF for Multiple Web Policies

Agents in the facilitator provide policy interchange to avoid possibly inconsistent or ambiguous syntax and semantics between source and target policies.

A. Meta-PIF

We envision several important issues in the design of agents while using SemPIF as a mediation architecture to enforce policy management services, such as policy sequencing, adding, deleting, merging, etc.

- In the SemPIF architecture, agents use PIF to provide basic interchange services of various policy languages.
- The basic vocabularies of PIF for interchange of policies are specified in the various REL policy languages, such as P3P or ODRL. They are $\texttt{principal}, \texttt{subject}(\texttt{owner}), \texttt{object}(\texttt{user}), \texttt{resource}(\texttt{asset}), \texttt{right}, \texttt{obligation}, \texttt{purpose}$, and $\texttt{condition}$. In addition, access right vocabularies for privacy protection and DRM are different. We have $\{\texttt{collect}, \texttt{retain}, \texttt{disclose}\}$, etc. for privacy protection and we have $\{\texttt{download}, \texttt{view}, \texttt{print}\}$, etc. for DRM.
- Most of the basic vocabularies for meta-PIF are the same as PIF's except some of them are directly related to

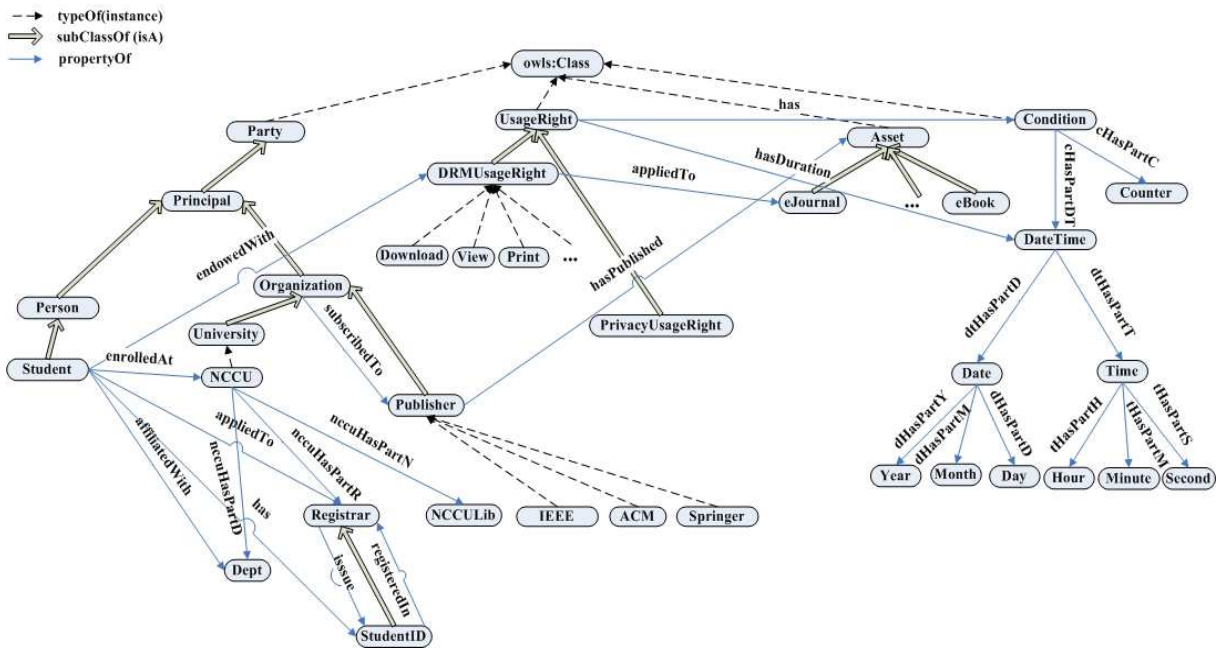

Fig. 5. A PIF-based ontology for DRM policies

PIF-based policies. The policy itself is introduced as a resource with respective users, rights, and conditions, etc. for agents to enforce its policy management services.

- Meta-PIF is a meta-policy language for PIF and only provides management services for PIF-based policies. If meta-PIF attempts to provide an interchange format for different meta-policies in PIF, then we also have to provide policy management interoperability services for different policy languages. This requires further study.

B. Agents in the facilitator enable meta-PIF policies

We use P3P basic vocabularies to specify data `owner` (or `subject`), `user` (or `object`), `type`, `right`, `obligation` as ontology classes with associated properties to formalize the semantics of privacy protection [10]. Furthermore, we also use Datalog-based rules to decide whether a Web server is allowed to `collect`, `retain`, or `disclose` a particular client's profiles and digital traces. Policies are defined as a combination of $\mathcal{O} + \mathcal{R}$. In order to unify policies from a client and a server, we allow agents in the facilitator to collect client and server's ontologies, and to enable SemPIF policy transformation and management services shown as follows:

1) **Ontologies mapping and aligning**
We map and align vocabularies from domain dependent ontologies of DRM and privacy protection policies. In Section III scenario, the vocabularies of class "$\texttt{Student}, \texttt{Publisher}$" in $\texttt{policy}(\texttt{drm1} - \texttt{IEEE})$ and $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$ correspond to "$\texttt{WebClient}, \texttt{WebServer}$" vocabularies of class in $\texttt{policy}(\texttt{pp3} - \texttt{John})$ to $\texttt{policy}(\texttt{pp4} - \texttt{John})$. Furthermore, we align the ontology schemas constructed with the vocabularies of class and property.

2) **Semantics mediation and unification**
We mediate and unify the semantic differences of vocabularies and schemas in the ontologies belonging to different protection policies. For example, a condition of $\texttt{Retain}[\texttt{hasDuration} \rightarrow =\texttt{2Month}]$ in the $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$ corresponds to a condition of "retention period less than fourteen days" in the $\texttt{policy}(\texttt{pp4} - \texttt{John})$.

3) **Conflicts resolving**
Agents initiate the reconciliation processes between conflicting policies using the meta-PIF framework. In this example, IEEE declares its intention to collect, retain, and disclose a Web user's data in the $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$ for two months. The data include a Web user's profiles and digital traces. Web user John does not allow an IEEE Web server to disclose his personal profile to the other partners. Thus, policies between $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$ and $\texttt{policy}(\texttt{pp3} - \texttt{John})$, $\texttt{policy}(\texttt{pp4} - \texttt{John})$ are inconsistent. Agents enable a policy priority-setting with meta-PIF-based policies to avoid the policy conflicts. In this example, an agent gives a higher priority to a client's $\texttt{policy}(\texttt{pp3} - \texttt{John})$ and $\texttt{policy}(\texttt{pp5} - \texttt{John})$ than to a server's $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$. The defeasible logic of a meta-PIF's expression, $\texttt{Overrides}(\texttt{policy}(?\texttt{pid1}), \texttt{policy}(?\texttt{pid2}))$, for resolving conflicts of policies is a possible solution, where $\texttt{policy}(?\texttt{pid1})$ is bound to $\texttt{policy}(\texttt{pp3} - \texttt{John})$ and $\texttt{policy}(\texttt{pp4} - \texttt{John})$; $\texttt{policy}(?\texttt{pid2})$ is bound to $\texttt{policy}(\texttt{pp1} - \texttt{IEEE})$. This negotiation protocol requires further study.

V. Related Work

REL is a subset of the PIF layers. FOL-semantics-enabled policy models for RELs have been proposed to specify the semantics of ODRL, XrML, and P3P [23] [24] [25]. However, it is still unclear how to design semantics-enabled policy languages from the FOL-enabled RELs to allow policies to be machine readable and understandable on the Web.

Tonti et. al. compared the three policy languages KAoS, Rei, and Ponder w.r.t. the representation and reasoning of specific policies [4]. The policy semantics of KAoS and Rei came from DL-based ontology. Rei has a policy management services framework for agents to manage policies but agents still cannot interoperate and cooperate with other agents across different frameworks. Moreover, policies created from LP-based policy languages, such as EPAL [15], were not able to interoperate and cooperate with the DL-based policies. We need a *de facto* standard policy interchange language as attempted by the W3C PLING[4] and with OMG's SBVR[5] to achieve policy interoperability.

The idea of meta-policies was proposed almost two decades ago [7]. It was used for policy management services in the Rei and Protune frameworks [5] [3]. In the Rei framework, the authors tried to propose a policy interchange mechanism instead of using a single policy language for describing all policies. Thus, SemPIF can be seen as bringing the objective of the Rei framework is close to the Semantic Web. In the Protune framework, meta-policies provide a simple means to specify which parts of a policy are sensitive, and how application-specific atomic conditions are to be verbalized in the documentation. However, predating SemPIF, the Rei and Protune frameworks did not show yet how a semantics-enabled policy layered architecture can be compatible with the current Semantic Web architecture.

VI. Conclusion and Future Work

We propose a semantics-enabled policy architecture, SemPIF, which extends W3C's Semantic Web layered architecture. We have introduced the SemPIF architecture as a 4-layer framework, i.e., UNL, PIF, PPD, and DSA. A meta-PIF layer is also introduced, side by side with the corresponding PIF, allowing agents in the facilitator to provide uniform services of interchange, reconciliation, and combination of policies from various domains on the Web. A scenario of employing SemPIF for DRM and privacy protection policies on digital library subscription services is described to demonstrate the feasibility of the SemPIF architecture. Future work include refining the PIF and meta-PIF languages to enable a multiple Web policies system on the Web.

Acknowledgements

This research was partially supported by the NSC Taiwan under Grant No. NSC 95-2221-E004-001-MY3, NSC 98-2918-E-004-003, and NSC 98-2221-E-004-009.

[4]Policy Interchanges Interest Group - PLING, http://www.w3.org/Policy/pling.

[5]Semantics of Business Vocabulary and Business Rules (SBVR), http://www.omg.org/spec/SBVR/1.0/.

References

[1] S. Bechhofer et al., "OWL web ontology language reference", Tech. Rep., W3C, Feb. 2004.

[2] H. Boley et al., "Rule interchange on the web", in *Reasoning Web 2007, Third International Summer School*, Dresden, Germany, Sep. 2007, LNCS 4636, Springer.

[3] L. Kagal et al., "Using semantic web technologies for policy management on the web", in *21st National Conference on Artificial Intelligence (AAAI)*. July 2006, AAAI.

[4] G. Tonti et al., "Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rei, and Ponder", in *2nd International Semantic Web Conference (ISWC) 2003*, 2003, LNCS 2870, pp. 419–437.

[5] P. Bonatti and D. Olmedilla, "Policy language specification, enforcement, and integration. project deliverable D2, working group I2", Tech. Rep., REWERSE, 2005.

[6] F. P. Patel-Schneider and I. Horrocks, "A comparison of two modelling paradigms in the semantic web", *Journal of Web Semantics*, pp. 240–250, 2007.

[7] H. Hilary Hosmer, "Metapolicies I", *ACM SIGSAC Review*, vol. 10, no. 2-3, pp. 18–43, 1992.

[8] Jos de Bruijn, "RIF RDF and OWL compatibility", Tech. Rep., W3C, Oct. 2009, http://www.w3.org/TR/rif-rdf-owl/.

[9] Y. J. Hu, "Semantic-driven enforcement of rights delegation policies via the combination of rules and ontologies", in *Workshop on Privacy Enforcement and Accountability with Semantics in conjunction with ISWC+ASWC'07*, 2007.

[10] Y. J. Hu, H. Y. Guo, and G. D. Lin, "Semantic enforcement of privacy protection policies via the combination of ontologies and rules", in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*, Taichung, Taiwan, June 2008.

[11] I. Horrocks et al., "SWRL: A semantic web rule language combining OWL and RuleML", 2004.

[12] N. B. Grosof et al., "Description logic programs: Combining logic programs with description logic", in *World Wide Web 2003*, Budapest, Hungary, 2003, pp. 48–65.

[13] M. F. Donini et al., "*AL*-log: Integrating datalog and description logics", *Journal of Intelligent Information Systems*, vol. 10, no. 3, pp. 227–252, 1998.

[14] B. Motik, U. Sattler, and R. Studer, "Query answering for OWL-DL with rules", in *3rd International Semantic Web Conference (ISWC) 2004*. 2004, LNCS 3298, pp. 549–563, Springer.

[15] G. Karjoth and M. Schunter, "A privacy policy model for enterprises", in *15th IEEE Computer Security Foundations Workshop (CSFW)*. June 2002, IEEE.

[16] E. Rissanen, "eXtensible Access Control Markup Language (XACML) ver. 3.0", May 2007.

[17] A. H. Anderson, "A comparison of two privacy policy languages: EPAL and XACML", in *Proceedings of the 3rd ACM Workshop on Secure Web Services (SWS'06)*. 2006, pp. 53–60, ACM.

[18] L. Cranor et al., "The platform for privacy preferences (P3P) 1.0 (P3P 1.0) specification", 2002, http://www.w3.org/P3P/.

[19] Inc. ContentGuard, "XrML: The digital rights language for trusted content and services", Tech. Rep., ContentGuard Inc., 2002.

[20] S. Guth and R. Iannella, "Open Digital Rights Language (ODRL) version 2", ODRL initiative working draft, The ODRL Initiative, February 2005.

[21] E. J. Cohen, "DRM and privacy", *Commun. ACM*, vol. 46, no. 4, pp. 47–49, 2003.

[22] D. J. Weitzner et al., "Creating a policy-aware web: Discretionary, rule-based access for the world wide web", in *Web and Information Security*, E. Ferrari and B. Thuraisingham, Eds., pp. 1–31. Idea Group Inc., 2006.

[23] Y. J.and Vicky Weissman Halpern, "A formal foundation for XrML", *Journal of the ACM*, vol. 55, no. 1, pp. 1–42, 2008.

[24] N. Li, T. Yu, and A. I. Antón, "A semantics-approach to privacy languages", *Computer Systems and Engineering (CSSE)*, vol. 21, no. 5, Sep. 2006.

[25] R. Pucella and V. Weissman, "A formal foundation for ODRL", arXiv:cs/0601085v1, Cornell University, January 2006, http://arxiv.org/abs/cs/0601085.